Cyber Threat Framework Version 4.0 Lexicon

The Cyber Threat Framework Lexicon is meant to be a flexible and open document. Our goal is to provide enough content and guidance to allow users to appropriately and repeatably categorize data without producing a massive document covering every conceivable possibility at the “Action” and “Indicator” level.

We solicit your comments and feedback on content, accuracy, and usability as a means to continually improve its content and utility.

Recommended changes must be unencumbered (e.g., non-proprietary or copyrighted) as they will be shared openly.

Terms				Definitions
Layer 1 Stages	**layer 2 Objectives**	**Layer 3 Actions**	**Layer 4 Indicators**	
stages				The progression of cyber threat actions over time to achieve objectives.
	objectives			The purpose of conducting an action or a series of actions.
		actions		Activity and associated resources used by a threat actor to satisfy an objective.
			indicators	Exemplars of discrete, measurable, cyber threat data, i.e., presence of malicious software, named Malware, and/or reported instances of malicious actions or activities, that connotes a threat actor's attempt to take or having taken an action, or to achieve an objective.

Preparation	Activities undertaken by a threat actor, their leadership and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, and strategy; identify potential victims and attack vectors; securing resources and develop capabilities; assess intended victim's cyber environment; and define measures for evaluating the success or failure of threat activities.			
	Plan activity			Steps taken by a threat actor before conducting malicious cyber activity to: define intent; establish policy limitations; identify funding; coordinate intended activities; establish initial objectives and parameters for measuring progress/success towards meeting them; and the steps taken to update plans, activities, and requirements based upon insights gained during the eventual victim engagement.
		Identify intended target(s) and the purpose for the malicious cyber activity		The intitial step in the planning process that produces a list of intended victim(s), and defines the intent for and desired outcome of the malicious cyber activity.
		Outline where and how the malicious activity is to be conducted		Actions taken by a threat actor (individual, team or government-sponsored agency), their sponsor and/or leadership to establish the overall strategy for, policy limitations of, and the requisite resources and capabilities needed to conduct the intended malicious cyber activity, (e.g., information needs, resources and capabilities, and partnerships), along with the criteria for evaluating the eventual success/failure (measures of performance, merit, and effectiveness [MoP/MoM/MoE]) of the activity.
		Establish a projected timeline for the malicious activity		The last step in the initial planning process in which the threat actor establishes a projected time for executing the planned malicious activity.

	Conduct research and analysis			Steps taken by the threat actor (without engaging the intended victim(s)) to gather additional information to: develop, expand upon, and/or validate planning assumptions concerning strengths, vulnerabilities, and potential attack vectors for the intended victim(s); to support activity risk assessments; to refine the list of intended target(s); and to finalize objectives for satisfying the original intent and achieving the intended outcomes.
	Develop resources and capabilities			Steps taken by the threat actor to secure the requisite resources (funding, people), and acquire the capabilities (technology, processes, tools, infrastructure), and partnerships necessary for conducting the planned cyber threat activity, and for ascertaining its success/failure in achieving the desired objectives/outcomes.
		Dedicate resources		Steps taken to secure funding and to recruit/train the people (on cyber activities, targeting, and data analysis) required to support/conduct intended cyber activities.
		Create capabilities necessary to accomplish the intended cyber activity		Steps taken to define, develop, acquire, and test the selected technology, processes, and tools, and acquire the facilities and infrastructure required to conduct the intended cyber activity.
		Outline where and how the malicious activity is to be conducted		Steps taken to establish relationships with individuals, groups or governments, to acquire or provide co-production and/or contract development of technology, processes and/or tools for use in the intended cyber activity, and to provide proxy support for compromising the intended victim's supply chain.
	Acquire victim specific knowledge			Steps taken by the threat actor prior to gaining access to an intended victim's computer(s), information system(s), network(s), and/or data stores, but just prior to execution of the planned cyber activity, to gather through physical/electronic observation (i.e., port scanning) or social media surveys, the latest details on the activities, characteristics, resources and perceived vulnerabilities of the intended victim to validate/confirm final planning assumptions.
	Complete preparation			Warehousing malicious cyber capabilities in/on threat actor internally owned or externally acquired storage locations, whether as electronic media or physical hardware (i.e., removable media, bundled hardware/firmware/software corrupted through a cooperative supply chain) for future deplyment, and issuing final instructions to those that will conduct the planned malicious activity.

Engagement	Threat actor activities taken prior to gaining but with the intent to gain unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s), and/or data stores.			
	Deploy capability			Steps taken to position malicious content for operational employment, e.g., place corrupted firmware in commercial products.
	Interact with intended victim			Contact between threat actor and intended victim in an attempt to establish an opportunity to or to gain direct access to victim's computer system/network.
		Persuade people to act on threat actor's behalf		Activities like social engineering that psychologically manipulate the target audience (i.e., insiders, outsiders with potential influence) to get them to perform supporting actions or divulge key information that enables subsequent malicious activity.
		Obtain a legitmate user account		Steps taken to openly gain authorized access to the victim's enviornment, e.g., submit an open request, impersonate a valid user, use hijacked credentials, or spoofiing the intended victim's computer, information system and/or network into believing the threat actor is a legitimate user.
	Exploit vulnerabilities			Steps taken to leverage deficiencies, vulnerabilities, gaps, and/or shortfalls (e.g., zero day exploits, malicious SQL injects, cross-site scripting) in the intended victim's computer(s), network(s), and/or information system(s) in an attempt to gain unauthorized access.
	Deliver malicious capability			Electronic or physical activities that expose malicious content to the intended victim that results in a physical or electronic presence but which does not activate the malicious content, e.g., send an email to intended victim with malicious attachment, distribute removable media containing Malware.

Presence	Actions taken by the threat actor once unauthorized access to victim(s)' physical or virtual computer or information system has been achieved that establishes and maintains conditions or allows the threat actor to perform intended actions or operate at will against the host physical or virtual computer or information system, network and/or data stores.			
	Establish controlled access			Activities (automated or manual) intended to gain unauthorized control (violate the confidentiality) of the intended victim's computer(s), information system(s), and/or network(s) to allow the threat actor to direct or conduct enabling or malicious activity.
		Manage deployed capability		Steps taken by a threat actor to activate, calibrate, request/status, reconfigure or deactive deployed Malware, to create conditions that support intended or to initiate malicious activity on victim's computer(s) and/or network(s).
		Establish illicit user access		Activitites conducted to gain access to and/or permissions for the intended victim(s)' computer, information systems or data stores, e.g., credential theft, impersonating a known user, spoofing the intended victim into thinking the threat actor is someone else, or by using existing capabilities (i.e., protocol manipulation, application/script/shell exploits, impersonation/spoofing) to authorize account activities for which legitimate access would not normally be granted.
		Employ anti-intrusion detection system measures		Threat actor actions (e.g., installing rootkits) taken to avoid detection by victim's intrusion detection capabilities/systems.
		Employ anti-forensics measures		Threat actor actions to destroy or obfuscate data that would indicate their presence on victim's computer(s), information system(s), and/or network(s), and thereby render victim-initiated forensic analysis difficult or impossible.
	Hide			Steps taken by a threat actor or Malware to avoid detection (e.g., obfuscation, masquerading, indicator manipulation, creation of unique libraries) on the victim's computer(s), information system(s), and/or network(s).
		Employ anti-intrusion detection system measures		Threat actor actions (e.g., installing rootkits) taken to avoid detection by victim's intrusion detection capabilities/systems.
		Employ anti-forensics measures		Threat actor actions to destroy or obfuscate data that would indicate their presence on victim's computer(s), information system(s), and/or network(s), and thereby render victim-initiated forensic analysis difficult or impossible.

	Expand presence			Steps taken by a threat actor to broaden their initial footprint (measured in terms of authorizations and/or system capabilities) on the victim's computer(s), information system(s), and/or network(s), to support/conduct additional malicious activity.
		Increase user privileges		Steps taken by the threat actor actions to exploit a bug, design flaw, or configuration oversight in an operating system or software application on a victim's computer(s), information system(s), and/or network(s) to gain access to resources that are unavailable to normal users, or beyond the level at which the initial threat actor footprint was established.
		Move laterally		Steps taken by the threat actor to explore the victim's computer(s), information system(s), and/or network(s), from the original point of entry and privilege level (or subsequently using modified authorities/system capabilities), in order to maintain a presence or gain access to additional capabilities, networks, hosts, and/or data.
		Compromise additional infrastructure		Activities by the threat actor to place corrupted/malicious code, firmware, and/or hardware in the intended victim's system environment.
	Refine focus of activity			Steps taken by the threat actor confirm the existence and validity of the intended victim's data, information, and/or system capabilities, and/or identify additional potential victims and their data, computer(s), and/or information system(s), and that the available malicious tools/processes will achieve the intended outcome/results.
	Establish persistence			Steps taken by the threat actor (electronically or physically) to preserve, obfuscate, or increase their footprint or capabilities on a victim's computer(s), information system(s), and/or network(s), e.g., additions to or modification of the existing operating system or enterprise capabilities (e.g., Windows software services, Master Boot Record), or the implant of additional malicious software.

Effect/Consequence	Outcomes of threat actor actions on a victim's physical or virtual computer or information system(s), network(s), and/or data stores.			
	Enable other activities			Measurable cyber threat activities that indicate, identify and/or establish a foundation for (to include the conduct of effects assessments) subsequent actions against a victim's data, computer(s) and/or information systems, e.g., establish a command and control node or hop point, incorporates the victim's computer/information systems in a botnet, or exfiltrate user password and/or credentials. Analytic judgments or assessments are not included.
	Deny access			Steps taken by the threat actor to temporarily degrade, disrupt, or destroy access to, or 'encrypt for ransom', (violate the availability) a victim's physical or virtual computer or information system(s), network(s), communications capabilities, and/or data stores.
		Disrupt/degrade communication links		Steps taken by the threat actor to deny access to or operation of, to some degree and/or for a period of time, the victim's communications infrastructure.
		Conduct Denial of Service (DoS) and/or Distributed Denial of Service (DDoS) attack		Normal system activities directed at the victim's environment in a magnitude that overwhelms the normal operation of the victim's computer(s), network(s), and/or information system(s), thus severly limiting or precluding normal external access.
		Disrupt/degrade the network		Activities initiated by the threat actor alter the operation of, to some degree and/or for a period of time, the victim's information system network.
		Execute ransomware		Threat actor use of ransomware installed on victim's computer(s), network(s), and or information system(s) to deny target access to their automated systems and data until access key is provided.

	Extract data			Threat actor activities within the victim's resources to move data/data stores to an alternative location, either within the target's data stores, computers and/or systems, or external to them.
		Relocate and store data on victim's computer, information system(s), network(s), and/or data stores.		Steps taken by a threat actor from within the victim's resources to acquire, copy, accumulate, and move (stage) data/information on a target's data/data stores, computer(s), information system(s), or network(s) to a location or in a form not originally intended by the victim's established data management/software application processes.
		Exfiltrate data/information		The movement/removal of data/information (things of intrinsic value), either electronically or physically, from the victim's computer(s), information system(s), and/or network(s) environment by a threat actor without the data owner's permission and/or knowledge.
	Alter computer, network, and/or system behavior			Steps taken by the threat actor to change the behavior/outcomes/and interaction (violate the integrity) of the victim's computer(s), information system(s), and/or network(s).
		Change process run-state on victim system(s)		Steps taken by the threat actor to alter processes operating on the victim's computer(s), network(s), and/or information system(s), i.e., change to ready, running, blocked, terminated, kernal mode, user mode, to support or achieve desired threat actor outcomes.
		Change decisions		Steps taken by the threat actor to change/alter the process outcomes of victim's internal target computer(s), network(s), and/or information system(s).
		Change machine-to-machine (MtM) communications		Steps taken by the threat actor to alter communications between processes operating on the victim's computer(s), network(s) and/or information system(s), or between systems in the victim's environment, to achieve desired threat actor outcomes.
	Destroy hardware/software/data			Permanently, completely and irreparably damage a victim's physical or virtual computer or information system(s), network(s), and/or data stores, e.g., system administrators discover permanent unexplained damage to portions of the information system, system users discover data/files have been inappropriately corrupted or deleted.